

A STRUCTURAL APPROACH TO SUBSET-SUM PROBLEMS

VAN VU

ABSTRACT. We discuss a structural approach to subset-sum problems in additive combinatorics. The core of this approach are Freiman-type structural theorems, many of which will be presented through the paper. These results have applications in various areas, such as number theory, combinatorics and mathematical physics.

1. INTRODUCTION

Let $A = \{a_1, a_2, \dots\}$ be a subset of an additive group G (all groups discussed in this paper will be abelian). Let S_A be the collection of subset sums of A

$$S_A := \left\{ \sum_{x \in B} x \mid B \subset A, |B| < \infty \right\}.$$

Two related notions that are frequently considered are

$$lA := \{a_1 + \dots + a_l \mid a_i \in A\}$$

$$l^*A := \{a_1 + \dots + a_l \mid a_i \in A, i \neq j\}.$$

We have the trivial relations

$$l^*A \subset lA \text{ and } \cup_l l^*A = S_A.$$

One can have similar definitions for A being a sequence (repetitions allowed).

Example.

$$A = \{0, 1, 4\}, G = \mathbf{Z}, 2A = \{0, 1, 2, 4, 5, 8\}, 2^*A = \{1, 4, 5\}, S_A = \{0, 1, 4, 5\}.$$

$$A = \{0, 1, 4\}, G = \mathbf{Z}_5, 2A = G, 2^*A = \{0, 1, 4\} = S_A.$$

V. Vu is supported by NSF Career Grant 0635606.

Now let A be a sequence:

$$A = \{1, 1, 9\}, G = \mathbf{Z}, 3A = \{3, 11, 19, 27\}, 3^*A = \{11\}, S_A = \{1, 1, 2, 9, 10, 11\}.$$

Notice that for a large l , lA can be significantly different from S_A and l^*A . In general, it is easier to handle than the later two.

Many basic problems in additive combinatorics have the following form:

*If A is sufficiently dense in G , then S_A (or l^*A or lA) contains a special element (such as 0 or a square), or a large structure (such as a long arithmetic progression G itself).*

The main question is to find the threshold for “dense”. As examples, we present below a few well-known results/problems in the area. In the whole paper, we are going to focus mostly on two special cases: (1) $G = \mathbf{Z}_p$, where \mathbf{Z}_p denotes the cyclic group of residues modulo a large prime p ; (2) $G = \mathbf{Z}$, the set of integers.

Following the literature, we say that A is *zero-sum-free* if $0 \notin S_A$. Furthermore, A is *complete* if $S_A = G$ and *incomplete* otherwise. The asymptotic notation is used under the assumption that $|A| \rightarrow \infty$.

A basic result concerning zero-sum-free sets is the following theorem of Olson [53] and Szemerédi [60] from the late 1960s, addressing a problem of Erdős and Heilbronn [23].

Theorem 1.1. (*Olson-Szemerédi*) *Let A be a subset of \mathbf{Z}_p with cardinality $C\sqrt{p}$, for a sufficiently large constant C . Then S_A contains zero.*

To see that order \sqrt{p} is necessary, consider $A := \{1, 2, \dots, n\}$, where $n \approx \sqrt{2p}$ is the largest integer such that $1 + \dots + n < p$.

Concerning completeness, Olson [52], proved the following result

Theorem 1.2. (*Olson*) *Any subset A of \mathbf{Z}_p with cardinality at least $\sqrt{4p-3} + 1$ is complete.*

To see that the bound is close to optimal, take $A := \{-m, \dots, -1, 0, 1, \dots, m\}$ where m is the largest integer such that $1 + \dots + m < \lfloor p/2 \rfloor$.

Another classical result concerning zero sums is that of Erdős-Ginburg-Ziv [42], again from the 1960s.

Theorem 1.3. (*Erdős-Ginburg-Ziv*) *If A is a sequence of $2p-1$ elements in \mathbf{Z}_p , then p^*A contains zero.*

This theorem is sharp by the following example: $A = \{0^{[p-1]}, 1^{[p-1]}\}$. Furthermore, instead of 0 and 1, one can use any two different elements of \mathbf{Z}_p . (Here and later $x^{[k]}$ means x appears with multiplicity k in A .)

Now we discuss two problems involving integers. Set $[n] := \{1, 2, \dots, n\}$. An old and popular conjecture concerning subset sums of integers is Folkman's conjecture, made in 1966 [25]. Folkman's conjecture is a strengthening of a conjecture by Erdős [20] about finding a necessary and sufficient condition for a sequence A such that S_A contains all but finite exception of the positive integers.

Conjecture 1.4. (*Folkman's conjecture*) *The following holds for any sufficiently large constant C . Let A be an strictly increasing sequence of positive integers with (asymptotic) density at least $C\sqrt{n}$ (namely, $|A \cap [n]| \geq C\sqrt{n}$ for all sufficiently large n). Then S_A contains an infinite arithmetic progression.*

Cassels [10] and Erdős [20] showed that density \sqrt{n} is indeed needed; thus, Folkman's conjecture is sharp up to the value of C . For more discussion about Folkman's conjecture and its relation with Erdős' conjecture, we refer to [25] and the monograph [21] by Erdős and Graham.

Finally, a problem involving a non-linear relation, posed by Erdős in 1986 [19].

Problem 1.5. (*Erdős' square-sum-free problem*) *A set A of integers is square-sum-free if S_A does not contain a square. Find the largest size of a square-sum-free subset of $[n]$.*

Erdős observed that one can construct such a square-sum-free subset of $[n]$ with at least $\Omega(n^{1/3})$ elements. To see this, consider $A := \{q, 2q, \dots, kq\}$ with q prime, $(k+1)k < 2q$, $kq \leq n$. Since the sum of all elements of A is less than q^2 , S_A does not contain a square. Erdős [19] conjectured that the truth is close to this lower bound.

Problems involving subset sums such as the above (and many others) have been attacked, with considerable success, using various techniques: combinatorial, harmonic analysis, algebraic etc. The reader who is interested in these techniques may want to look at [3, 57, 64, 48] and the references therein.

The goal of this paper is to introduce the so-called “structural approach”, which has been developed systematically in recent years. This approach is based on the following simple plan

Step I: Force a structure on A . In this step, one tries to show the following: If A is relatively dense (close to the conjectured threshold but not yet there) and S_A does not contain the desired object, then A has a very special structure.

Alternately, one can try to

Step I': Find a structure in S_A . If A is relatively dense (again close to the conjectured threshold but not yet there) then S_A contains a special structure.

Step II: Completion. Since $|A|$ is still below the threshold, we can add (usually many) new elements to A . Using these elements together with the existing structure, one can, in most cases, obtain the desired object in a relatively simple manner.

The success of the method depends on the quality of the information we can obtain on the structure of A (or S_A) in Step I (or I'). In several recent studies, it has turned out that one can frequently obtain something close to a *complete characterization* of these sets. Thanks to these results, one is able to make considerable progresses on many old problems and also reprove and strengthen several existing ones (with a better understanding and a complete classification of the extremal constructions).

The rest of this paper is devoted to the presentation of these structural theorems and their representative applications.

2. FREIMAN'S STRUCTURAL THEOREM

A corner stone in additive combinatorics is the structural theorem of Freiman (some-time referred to as Freiman's inverse theorem), which writes down the structure of sets with small doubling.

A *generalized arithmetic progression* (GAP) of rank d in a group G is a set of the form

$$\{a_0 + a_1x_1 + \cdots + a_dx_d \mid M_i \leq x_i \leq N_i\},$$

where a_i are elements of G and $M_i \leq N_i$ are integers. It is intuitive to view a GAP Q as the image of the d -dimensional integral box $B := \{(x_1, \dots, x_d) \mid M_i \leq x_i \leq N_i\}$ under the linear map

$$\Phi(x_1, \dots, x_d) = a_0 + a_1x_1 + \cdots + a_dx_d.$$

We say that Q is *proper* if Φ is one-to-one. It is easy to see that if Q is a proper GAP of rank d and A is a subset of density δ of Q , then $|2A| \leq C(d, \delta)|A|$. Indeed,

$$|2A| \leq |2Q| \leq |2B| = 2^d|B| = 2^d|Q| \leq \frac{2^d}{\delta}|A|$$

since the volume of a box increases by a factor 2^d if its sizes are doubled.

Freiman's theorem shows that this is the *only* construction of sets with constant doubling.

Theorem 2.1. (*Freiman's theorem*) [27] *For any positive constant C , there are positive constants $d = d(C)$ and $\delta = \delta(C)$ such that the following holds. Let A be a finite subset of a torsion-free group G such that $|2A| \leq C|A|$. Then there is a proper GAP Q of dimension d such that $A \subset Q$ and $|A| \geq \delta|Q|$.*

Freiman theorem has been extended recently to the torsion case by Green and Ruzsa [35]. [64, Chapter 5] contains a detailed discussion of both theorems and related results.

One can use Freiman's theorem iteratively to treat the sumset lA , for $l > 2$. For simplicity, assume that $l = 2^s$ is a power of 2. Thus, the set $A_s := lA = 2^s A$ can be viewed as $2A_{s-1}$ where $A_{s-1} := 2^{s-1}A$. Using a multi-scale analysis combined with Freiman's theorem, one can obtain useful structural information about lA or A itself. For an example of this technique, we refer to [61] or [64, Chapter 12].

The treatment of l^*A and S_A is more difficult. However, one can still develop structural theorems in these cases. While the content of most theorems in this direction are quite different from that of Freiman's, they do bear a similar spirit that somehow the most natural construction happens to be (essentially) the only one.

3. STRUCTURE OF ZERO-SUM-FREE SETS

Let A be a zero-sum-free subset of \mathbf{Z}_p . We recall the example following Theorem 1.1. Let $A := \{1, 2, \dots, n\}$. If $1 + \dots + n < p$, then obviously S_A does not contain 0. This shows that a zero-sum-free set can have close to $\sqrt{2p}$ elements. In [61], Szemerédi and Vu showed that *having elements with small sum is essentially the only reason for a set to be zero-sum-free*. More quantitative versions of this statement were worked out in [49] and [50]. For example, we have [50, Theorem 2.2]

Theorem 3.1. *After a proper dilation (by some non-zero element), any zero-sum-free subset A of \mathbf{Z}_p has the form*

$$A = A' \cup A''$$

where the elements of A' (viewed as integers between 0 and $p-1$) are small, $\sum_{x \in A'} x < p$, and A'' is negligible, $|A''| \leq p^{6/13+o(1)}$.

One can perhaps improve the constant $6/13$ by tightening the analysis in [50]. It is not clear, however, what would be the best constant here. In most applications, it suffices to have any constant strictly less than $1/2$.

The dilation is necessary. Notice that if A is zero-sum-free (incomplete), then the set $A_x := \{xa | a \in A\}$ is also zero-sum-free (incomplete) for any $0 \neq x \in \mathbf{Z}_p$.

We can also prove similar results for lA and l^*A , and for A being a sequence (see [50] for details). In the rest of this section, we present few applications of these results.

3.2. The size of the largest zero-sum-free set in \mathbf{Z}_p . Let m_p denote the size of the largest zero-sum-free set in \mathbf{Z}_p . The problem of determining m_p was posed by

Erdős and Heilbronn [23] and has a long history. Szemerédi proved that $m_p \leq C\sqrt{p}$, for some sufficiently large C independent of p [60]. Olson showed that $C = 2$ suffices [53]. Much later, Hamidoune and Zémor [37] showed that $m_p \leq \sqrt{2p} + 5\log p$, which is asymptotically sharp. Using an earlier version of Theorem 3.1, Szemerédi, Nguyen and Vu [49] recently obtained the exact value of m_p .

Theorem 3.3. *Let n_p be the largest integer so that $1 + \dots + (n_p - 1) < p$.*

- *If $p \neq \frac{n_p(n_p+1)}{2} - 1$, then $m_p = n_p - 1$.*
- *If $p = \frac{n_p(n_p+1)}{2} - 1$, then $m_p = n_p$. Furthermore, up to a dilation, the only zero-sum-free set with n_p elements is $\{-2, 1, 3, 4, \dots, n_p\}$.*

The same result was obtained by Deshouillers and Prakash (personal communication by Deshouillers) at about the same time.

3.4. The structure of relatively large zero-sum-free sets. Let us now consider the structure of zero-sum-free sets of size close to $\sqrt{2p}$. Let $\|x\|$ denote the integer norm of x . In [15], Deshouillers proved

Theorem 3.5. *Let A be a zero-sum-free subset of Z_p of size at least \sqrt{p} . Then (after a proper dilation)*

$$\sum_{x \in A, x < p/2} \|x/p\| \leq 1 + O(p^{-1/4} \log p)$$

$$\sum_{x \in A, x > p/2} \|x/p\| \leq O(p^{-1/4} \log p).$$

Deshouillers showed (by a construction) that the error term $p^{-1/4}$ cannot be replaced by $o(p^{-1/2})$. Using an earlier version of Theorem 3.1, Nguyen, Szemerédi and Vu [49] improved Theorem 4.4 to obtain the best possible error term $O(p^{-1/2})$, under a stronger assumption on the size of $|A|$.

Theorem 3.6. *Let A be a zero-sum-free subset of Z_p of size at least $.99\sqrt{2p}$. Then (after a proper dilation)*

$$\sum_{x \in A, x < p/2} \|x/p\| \leq 1 + O(p^{-1/2})$$

$$\sum_{x \in A, x > p/2} \|x/p\| \leq O(p^{-1/2}).$$

The constant .99 is, of course, ad-hoc and can be improved by redoing the analysis carefully. On the other hand, it is not clear what the best assumption on $|A|$ should be.

3.7. Erdős-Ginburg-Ziv revisited. Using a version of Theorem 3.1 for sequences, Nguyen and Vu [50] obtained the following characterization for a sequence of size slightly more than p and does not contain a subsequence of p elements summing up to 0.

Corollary 3.8. [50, Theorem 6.2] *Let ε be an arbitrary positive constant. Assume that A is a p -zero-sum-free sequence and $p + p^{12/13+\varepsilon} \leq |A| \leq 2p - 2$. Then A contains two elements a and b with multiplicities m_a, m_b satisfying $m_a + m_b \geq 2(|A| - p - p^{12/13+\varepsilon})$.*

The interesting point here is that the structure kicks in very soon, when A has just slightly more than p elements. Few years ago, Gao, Panigrahi, and Thangdurai [43] proved a similar statement under the stronger assumption that $|A| \geq 3p/2$.

It is easy to deduce Erdős-Ginburg-Ziv theorem from Corollary 3.8, together with a complete characterization of the extremal sets. The reader may want to consider as an exercise or check [50] for details.

4. INCOMPLETE SETS

Now we turn our attention to incomplete sets, namely sets A where $S_A \neq \mathbf{Z}_p$. The situation here is very similar to that with zero-sum-free sets. Szemerédi and Vu [61] showed that *having elements with small sum is essentially the only reason for a set to be incomplete*. More quantitative versions of this statement were worked out in [49] and [50]. For example, in [50], the following analogue of Theorem 3.1 was proved

Theorem 4.1. *After a proper dilation (by some non-zero element), any incomplete subset A of \mathbf{Z}_p has the form*

$$A = A' \cup A''$$

where the elements of A' are small (in the integer norm), $\sum_{x \in A'} \|x/p\| < 1$ and A'' is negligible, $|A''| \leq p^{6/13+o(1)}$.

The reader can find similar results for lA and l^*A and for A being a sequence in [50]. We next discuss some applications of these results.

4.2. The structure of relatively large incomplete sets. Theorem 4.1 enables us to prove results similar to those in the last section for incomplete sets. The problem of determining the largest size of an incomplete set in \mathbf{Z}_p was first considered by Erdős and Heilbronn [23] and essentially solved by Olson (Theorem 1.2). da Silva and Hamidoune [12] tightened the bound to $\sqrt{4p-7} + 1$, which is best possible. We are not going to go into these results here, but note that one can perhaps obtain a new proof (with a characterization of the extremal sets) using Theorem 4.1.

Concerning the structure of relatively large incomplete sets, Deshouillers and Freiman [17] proved

Theorem 4.3. *Let A be an incomplete subset of \mathbf{Z}_p of size at least $\sqrt{2p}$. Then (after a proper dilation)*

$$\sum_{x \in A} \|x/p\| \leq 1 + O(p^{-1/4} \log p).$$

They conjectured that the error term may be replaced by $O(\sqrt{p})$, which would be best possible due to a later construction of Deshouillers [16].

Using Theorem 4.1, Nguyen and Vu [50] confirmed this conjecture, provided that A is sufficiently close to $2\sqrt{p}$.

Theorem 4.4. *Let A be an incomplete subset of \mathbf{Z}_p of size at least $1.99\sqrt{p}$. Then (after a proper dilation)*

$$\sum_{x \in A} \|x/p\| \leq 1 + O(\sqrt{p}).$$

Similar to the constant .99 (in the previous section), the constant 1.99 is ad-hoc and can be improved by redoing the analysis carefully. On the other hand, it is not clear what the best assumption on $|A|$ is.

4.5. The structure of incomplete sequences. Let us now discuss (rather briefly) the situation with sequences. The main difference between sets and sequences is that a sequence can have elements with high multiplicities. It has turned out that when the maximum multiplicity of incomplete sequence A is determined, one can obtain strong structural information about A .

Let $1 \leq m \leq p$ be a positive integer and A be an incomplete sequence of \mathbf{Z}_p with maximum multiplicity m . Trying to make A as large as possible, we come up with the following example,

$$B_m = \{-n^{[k]}, (n-1)^{[m]}, \dots, -1^{[m]}, 0^{[m]}, 1^{[m]}, \dots, (n-1)^{[m]}, n^{[k]}\}$$

where $1 \leq k \leq m$ and n are the unique integers satisfying

$$2m(1 + 2 + \dots + n - 1) + 2kn < p \leq 2m(1 + 2 + \dots + n - 1) + 2(k+1)n.$$

It is clear that any subsequence of B_m is incomplete and has multiplicity at most m . In [50], we proved that any incomplete sequence A with maximum multiplicity m and cardinality close to $|B_m|$ is essentially a subset of B_m .

Theorem 4.6. *Let $6/13 < \alpha < 1/2$ be a constant. Assume that A is an incomplete sequence of \mathbf{Z}_p with maximum multiplicity m and cardinality $|A| = |B_m| - O((pm)^\alpha)$. Then after a proper dilation, we can have*

$$A = A' \cup A''$$

where $A' \subset B_m$ and $|A''| = O((pm)^{(\alpha+1/2)/2})$.

4.7. Counting problems. Sometime one would like to count the number of sets which forbid certain additive configurations. A well-known example of problems of this type is the Cameron-Erdős problem [11], which asked for the number of subsets of $[n] = \{1, 2, \dots, n\}$ which does not contain three different elements x, y, z such that $x + y - z = 0$. Cameron and Erdős noticed that any set of odd numbers has this property. Thus, in $[n]$ there are at least $\Omega(2^{n/2})$ subsets with the required property. They conjectured that $2^{n/2}$ is the right order of magnitude. There were several partial results [2, 9, 22] before Green settled the conjecture [34].

Using structural theorems such as Theorem 3.1, one can obtain results of similar spirit for the number of zero-sum-free or incomplete sets and sequences. For example, using an earlier version of Theorem 3.1 and standard facts from the theory of partitions [1], Szemerédi and Vu [61] proved

Corollary 4.8. *The number of incomplete subsets of \mathbf{Z}_p is $\exp((\sqrt{\frac{2}{3}}\pi + o(1))\sqrt{p})$.*

Using Theorem 4.6, one obtains the following generalizations [50].

Corollary 4.9. *The number of incomplete sequences A with highest multiplicity m in \mathbf{Z}_p is $\exp((\sqrt{(1 - \frac{1}{m+1})\frac{4}{3}}\pi + o(1))\sqrt{p})$.*

It is an interesting question to determine the error term $o(1)$.

5. INCOMPLETE SETS IN A GENERAL ABELIAN GROUP

Let us now consider the problem of finding the largest size of an incomplete set in a general abelian group G , which we denote by $\text{In}(G)$ in the rest of this section. The situation with a general group G is quite different from that with \mathbf{Z}_p , due to the existence of non-trivial subgroups. It is clear that any such subgroup is incomplete. Thus, $\text{In}(G) \geq h$, where h is the largest non-trivial divisor of $|G|$. The intuition behind the discussion in this section is that *a large incomplete set should be essentially contained in a proper subgroup*.

In 1975, Diderrich [13] conjectured that if $|G| = ph$, where $p \geq 3$ is the smallest prime divisor of $|G|$ and h is composite, then $c(G) = h + p - 2$. (The cases where $p = 2$ or h is a prime is simpler and were treated earlier, some by Diderrich himself

[13, 47, 14].) Diderich's conjecture was settled by Gao and Hamidoune in 1999 [29].

The following simple fact explains the appearance of the term $p - 2$.

Fact. If $S_{A \cap H} = H$ for some maximal subgroup H of (prime) index q , then $|A| \leq |H| + q - 2$.

To verify this fact, notice that A/H is a sequence in the group \mathbf{Z}_q . It is easy to show (exercise) that if B is a sequence of $q - 1$ non-zero elements in \mathbf{Z}_q , then $S_B \cup \{0\} = \mathbf{Z}_q$.

We say that subset A of G is *sub-complete* if there is a subgroup H of prime index such that $S_{A \cap H} = H$.

Once we know that an incomplete set A is sub-complete, we can write down its structure completely. There is a subgroup H with prime index q such that $|A \setminus H| \leq q - 2$, and the sequence A/H is incomplete in \mathbf{Z}_q . (The structure of such a sequence was discussed in the previous section.) It is natural to pose the following

Problem 5.1. *Find the threshold for sub-completeness.*

Recently, Gao, Hamidoune, Lladó and Serra [30] showed (under some weak assumption) that any subset of at least $\frac{p}{p+2}h + p$ elements is sub-complete. Furthermore, one can choose H to have index p , where p is the smallest prime divisor of $|G|$. Vu [68] showed (again under some weak assumption) that $\frac{5}{6}h$ is sufficient to guarantee sub-completeness. It is not clear, however, what the sharp bound is.

The situation is much better if we assume that $|G|$ is sufficiently composite. In particular, if the product of the two smallest prime divisors of $|G|$ is significantly smaller than $\sqrt{|G|}$, then one can determine the sharp threshold for sub-completeness.

Theorem 5.2. [68] *For any positive constant δ there is a positive constant $D(\delta)$ such that the following holds. Assume that $|G| = p_1 \dots p_t$, where $t \geq 3$ and $p_1 \leq p_2 \dots \leq p_t$ are primes such that $p_1 p_2 \leq \frac{1}{D(\delta)} \sqrt{|G| / \log |G|}$. Then any incomplete subset A of G with cardinality at least $(1 + \delta) \frac{n}{p_1 p_2}$ is subcomplete. Furthermore, the lower bound $(1 + \delta) \frac{n}{p_1 p_2}$ cannot be replaced by $\frac{n}{p_1 p_2} + n^{1/4 - \alpha}$, for any constant α .*

6. STRUCTURES IN S_A

As mentioned in the introduction, an alternative way to implement our plan is to find a structure in S_A rather than in A (Step I'). A well-known result concerning the structure of S_A is the following theorem, proved by Freiman [28] and Sárközy [55] independently.

Theorem 6.1. *There are positive constants C and c such that the following holds for all sufficiently large n . Let A be a subset of $[n] := \{1, \dots, n\}$ with at least $C\sqrt{n \log n}$ elements. Then S_A contains an arithmetic progression of length $c|A|^2$.*

It is clear that the bound on the length of the arithmetic progression (AP) is optimal, as one can take A to be an interval. The lower bound on $|A|$, however, can be improved to $C\sqrt{n}$, as showed by Szemerédi and Vu [62].

Theorem 6.2. *There are positive constants C and c such that the following holds for all sufficiently large n . Let A be a subset of $[n] := \{1, \dots, n\}$ with at least $C\sqrt{n}$ elements. Then S_A contains an arithmetic progression of length $c|A|^2$.*

The assumption $|A| \geq C\sqrt{n}$ is optimal, up to the value of C , as one can construct a set $A \subset [n]$ of $\epsilon\sqrt{n}$ elements, for some small constant ϵ , such that S_A does not contain any arithmetic progression of length larger than $n^{3/4}$ (see [62] or [63, Section 3.4]).

Theorem 6.2 can be extended considerably. Szemerédi and Vu [63] showed that for any set $A \subset [n]$ and any integer l such that $l^d|A| \geq n$ for some constant d , the sumset l^*A contains a large proper generalized arithmetic progression (GAP). The parameters of this GAP is optimal, up to a constant factor (see [63, Section 3] for more details).

Theorem 6.3. [63, Theorem 7.1] *For any fixed positive integer d there are positive constants C and c depending on d such that the following holds. For any positive integers n and l and any set $A \subset [n]$ satisfying $l^d|A| \geq Cn$, l^*A contains a proper GAP of rank d' and volume at least $cl^{d'}|A|$, for some integer $1 \leq d' \leq d$.*

There are variants of Theorem 6.3 for finite fields, and also for sums of different sets (see [63, Section 5] and [63, Section 10]). In the following subsections, we discuss few applications of Theorems 6.2 and 6.3.

6.4. Folkman conjectures on infinite arithmetic progressions. Let us recall to the conjecture of Folkman, mentioned in the introduction.

Conjecture 6.5. *(Folkman's conjecture) The following holds for any sufficiently large constant C . Let A be an strictly increasing sequence of positive integers with (asymptotic) density $A(n)$ at least $C\sqrt{n}$ (namely $A(n) := |A \cap [n]| \geq C\sqrt{n}$ for all sufficiently large n). Then S_A contains an infinite arithmetic progression.*

Folkman [25] showed that the conjecture holds under a stronger assumption that $A(n) \geq n^{1/2+\epsilon}$, where ϵ is an arbitrarily small positive constant. (An earlier result of Erdős [20] on a closely related problem can perhaps be adapted to give a weaker bound $n^{(\sqrt{5}-1)/2}$.) Hegyvári [45] and Łuczak and Schoen [46], independently, reduced the density $n^{1+\epsilon}$ to $C\sqrt{n \log n}$, using Theorem 6.1.

Using the stronger Theorem 6.2, together with some additional arguments, Szemerédi and Vu [62] proved the full conjecture.

Theorem 6.6. *Conjecture 6.5 holds.*

In the same paper [25], Folkman also made a related conjecture for increasing, but not strictly increasing sequences. Let $A(n)$ now be the number of elements of A (counting multiplicities) at most n .

Conjecture 6.7. (*Folkman's second conjecture*) *The following holds for any sufficiently large constant C . Let A be an increasing sequence of positive integers with such that $A(n) \geq Cn$ for all sufficiently large n . Then S_A contains an infinite arithmetic progression.*

Despite the huge change from \sqrt{n} to n in the density bound, this conjecture is also sharp [25], and (for some time) appeared more subtle than the first one (see a discussion in [21, Chapter 6]). Folkman [25] proved the conjecture under the stronger assumption that $A(n) \geq n^{1+\varepsilon}$. It does not seem that one can obtain the analogue of Hegyvári and Łuczak-Schoen results due to the lack of a "sequence" variant of Theorem 6.1. However, the method in [63] is sufficiently robust to enable one to obtain such a variant for the stronger Theorem 6.2. With the help of this result, one can settle Conjecture 6.7

Theorem 6.8. [63, Section 6] *Conjecture 6.7 holds.*

The strategy for the proofs of Theorems 6.6 and 6.8 is the following. We first find a sufficient condition for a sequence A such that S_A contains an infinite AP.

We say that an infinite sequence A admits a *good* partition if it can be partitioned into two subsequences A' and A'' with the following two properties

- There is a number d such that $S_{A'}$ contains an arbitrary long arithmetic progression with difference d .
- Let $A'' = b_1 \leq b_2 \leq b_3 \leq \dots$. For any number K , there is an index $i(K)$ such that $\sum_{j=1}^{i-1} b_j \geq b_i + K$ for all $i \geq i(K)$.

Lemma 6.9. *If a sequence A admits a good partition then S_A contains an infinite AP.*

The second assumption is easy to satisfied given that A has proper density. Thus, the key is the first assumption. The main feature here is that in this assumption, we only need to guarantee the existence of long (but finite) APs. So, Theorem 6.2 and its variants can be used with full power to achieve this goal.

6.10. Erdős conjecture on square-sum-free sets. In this section, we return to Erdős conjecture on square-sum-free sets, mentioned in the introduction. Let $SF(n)$ denote the size of the largest subset A of $[n]$ such that S_A does not contain a square (or A is square-sum-free). Erdős [19] observed that $SF(n) = \Omega(n^{1/3})$ and conjectured that the truth is close to this lower bound. Since then, there have been several attempts on his conjecture. Alon [4] proved that $SF(n) = O(\frac{n}{\log n})$. In [40] Lipkin improved the bound to $SF(n) = O(n^{3/4+\varepsilon})$. Later, Alon and Freiman [5] obtained another improvement $SF(n) = O(n^{2/3+\varepsilon})$. About fifteen years ago, Sárközy [56] showed $SF(n) = O(\sqrt{n \log n})$.

Let us now address the problem from our structural approach point of view. Theorem 6.2 is no longer useful, as we are dealing with sets of size around $n^{1/3}$, way below the lower bound \sqrt{n} required in this theorem. Fortunately, we have a more general result, Theorem 6.3, which enables us to find structures in S_A for any set of size n^δ , for any constant δ . In particular, we can deduce from this theorem the following corollary.

Corollary 6.11. *There are positive constants C and c such that the following holds for all sufficiently large n . Let A be a subset of $[n]$ with cardinality at least $Cn^{1/3}$. Then S_A contains either an AP of length $c|A|^2$ or a proper GAP of rank 2 and volume $c|A|^3$.*

Combining this corollary with some number theoretic arguments, Nguyen and the author [51] can get close to the conjectured bound.

Theorem 6.12. *There is a constant C such that $SF(n) \leq n^{1/3} \log^C n$.*

We strongly believe that the log term can be removed. Details will appear elsewhere.

7. INVERSE LITTLEWOOD-OFFORD THEOREMS AND RANDOM MATRICES

In this final section, we discuss a problem with a slightly different nature. Let A be a sequence of non-zero integers. Now we are going to view S_A as a multi-set of 2^n elements. We denote by M_A be the largest multiplicity in S_A . For example, if $A = \{1, \dots, 1\}$, then $M_A = \binom{n}{\lfloor n/2 \rfloor} = \Theta(2^n / \sqrt{n})$.

The problem of bounding M_A originated from Littlewood and Offord's work on random polynomials [41]. In particular, they proved that $M_A = O(2^n \log n / \sqrt{n})$. The log term was removed by Erdős [18], who obtained a sharp bound for M_A . Many extensions of this result were obtained by various researcher: Erdős-Moser [24], Sárközy-Szemerédi [58], Katona [38] Kleitman [39], Halász [44], Griggs et. al. [36], Frankl-Füredi [26], Stanley [59] etc. Among others, it was showed that the bound on M_A keeps improving, if one forbids more and more additive structures in A . For example, Erdős and Moser [24] showed that if the elements of A are different (i.e., A is a set), then $M_A = O(2^n \log n / n^{3/2})$. In general, the following can be deduced from results of [44] (see also [64, Problem 7.2.8])

Theorem 7.1. *For any fixed integer k there is a constant C such that the following holds. Let $A = \{a_1, \dots, a_n\}$ and R_k be the number of roots of the equation*

$$\varepsilon_1 a_{i_1} + \dots + \varepsilon_{2k} a_{i_{2k}} = 0$$

with $\varepsilon_i = \pm 1$ and $i_1, \dots, i_{2k} \in [n]$. Then $M_A \leq Cn^{-2k-1/2} R_k$.

In [66], Tao and Vu introduced the notion of Inverse Littlewood-Offord theorems. The intuition here is that if M_A is large (of order $2^n / n^C$ for any constant C , say), then A should have a very strong structure.

The most general example we found with large M_A is the following. Let Q be a proper GAP of constant rank d and volume V . If A is a subset of Q , it is easy to show that $M_A = \Omega(\frac{1}{n^{d/2}V})$ (in order to see this, view the elements of S_A as random sums $\sum_{i=1}^n \xi_i a_i$ where a_i are elements of A and ξ_i are iid random variables taking values 0 and 1 with probability 1/2). Thus, if the volume of Q is small, then M_A is large.

In [66], Tao and Vu proved the inverse statement, asserting that *having A as a subset of a small GAP is essentially the only way to guarantee make M_A large.*

Theorem 7.2. [66] *For any constant C and ϵ there are constants B and d such that the following holds. Let A be a sequence of n elements in a torsion-free group G . If $M_A \geq 2^n/n^C$ for some constant C , then all but at most $n^{1-\epsilon}$ elements of A is contained in a proper GAP Q of rank d and cardinality n^B .*

In a more recent paper [67], the same authors obtained a (near) optimal relationship between the parameters C, ϵ, d and B . As a corollary, one can deduce (asymptotic versions of) many earlier results, such as Theorem 7.1. (In spirit, this process is somewhat similar to the process of using Theorem 3.1 to reprove, say, Erdős-Ginburg-Ziv theorem.)

We would like to conclude this survey with a rather unexpected application. Let us leave combinatorial number theory and jump to the (fairly remote) area of mathematical physics. In the 1950s, Wigner observed and proved his famous semi-circle law concerning the limiting distribution of eigenvalues in a *symmetric* random matrix [69]. A brother of this law, the so-called circular law for *non-symmetric* random matrices, has been conjectured, but remains open since that time.

Conjecture 7.3. (*Circular Law Conjecture*) *Let ξ be a random variable with mean 0 and variance 1 and M_n be the random matrix whose entries are iid copies of ξ . Then the limiting distribution of the eigenvalues of $\frac{1}{\sqrt{n}}M_n$ converges to the uniform distribution on the unit disk.*

Girko [31] and Bai [6] obtained important partial results concerning this conjecture. These results and many related results are carefully discussed in the book [7]. There has been a series of rapid developments recently by Götze-Tikhomirov [32, 33], Pan-Zhou [54], and Tao-Vu [65]. In particular, Tao and Vu [65] confirmed the conjecture under the slightly stronger assumption that the $(2 + \eta)$ -moment of ξ is bounded, for any $\eta > 0$.

Theorem 7.4. *The Circular Law holds (with strong convergence) under an additional assumption that*

$$\mathbf{E}(|\xi|^{2+\eta}) < \infty$$

for some fixed $\eta > 0$.

The key element of this proof is a variant of Theorem 7.2, which enables us to count the number of sequences A with bounded elements such that M_A (more precisely a continuous version of it) is large. For details, we refer to [65].

REFERENCES

- [1] G. E. Andrews, The theory of partitions. Cambridge university press, 1998.
- [2] N. Alon, Independent sets in regular graphs and sum-free subsets of abelian groups, *Israel Journal Math.* 73 (1991), 247-256.
- [3] N. Alon, Combinatorial Nullstellensatz, Recent trend in combinatorics (Mátraháza, 1995), *Combin. Probab. Comput.* 8 (1999), 7-29.
- [4] N. Alon, Subset sums. *Journal of Number Theory*, 27 (1987), 196-205.
- [5] N. Alon and G. Freiman, On sums of subsets of a set of integers, *Combinatorica*, 8 (1988), 297-306.
- [6] Z. D. Bai, Circular law, *Ann. Probab.* 25 (1997), no. 1, 494-529.
- [7] Z. D. Bai and J. Silverstein, Spectral analysis of large dimensional random matrices, Mathematics Monograph Series 2, Science Press, Beijing 2006.
- [8] A. Bialostocki and P. Dierker, On Erdős-Ginzburg-Ziv theorem and the Ramsey number for stars and matchings, *Discrete Mathematics*, 110, (1992), 1-8.
- [9] N. Calkin, On the number of sum-free sets, *Bull. London Math. Soc.* 22 (1990), 141-144.
- [10] J.W.S Cassels, On the representation of integers as the sums of distinct summands taken from a fixed set, *Acta Sci. Math. Szeged* 21 1960 111-124.
- [11] P. Cameron and P. Erdős, On the number of sets of integers with various properties, Number Theory (Banff, AB 1988), 61-79, de Gruyter, Berlin, 1990.
- [12] D. da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* 26 (1994), no. 2, 140-146.
- [13] G. T. Diderrich, An addition theorem for abelian groups of order pq , *J. Number Theory* 7 (1975), 33-48.
- [14] G. T. Diderrich and H. B. Mann, Combinatorial problems in finite Abelian groups, *Survey of combinatorial theory* (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971), pp. 95-100. North-Holland, Amsterdam, 1973.
- [15] J-M. Deshouillers, Quand seule la sous-somme vide est nulle modulo p . (French) [When only the empty subsum is zero modulo p] *J. Thor. Nombres Bordeaux* 19 (2007), no. 1, 71-79.
- [16] J-M Deshouillers, Lower bound concerning subset sum wich do not cover all the residues modulo p , *Hardy- Ramanujan Journal*, Vol. 28(2005) 30-34.
- [17] J-M Deshouillers and G. Freiman, When subset-sums do not cover all the residues modulo p , *Journal of Number Theory* 104(2004) 255-262.
- [18] P. Erdős, On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc.* 51 (1945), 898-902.
- [19] P. Erdős, Some problems and results on combinatorial number theory, Proceeding of the first China conference in Combinatorics, 1986.
- [20] P. Erdős, On the representation of large interges as sums of distinct summands taken from a fixed set, *Acta. Arith.* 7 (1962), 345-354.
- [21] P. Erdős and R. Graham, Old and new problems and results in combinatorial number theory. Monographies de L'Enseignement Mathematique [Monographs of L'Enseignement Mathematique], 28. Universit de Genve, L'Enseignement Mathematique, Geneva, 1980.
- [22] P. erdős and A. Granville, *Unpublished*.
- [23] P. Erdős and H. Heilbronn, On the addition of residue classes mod p , *Acta Arith.* 9 1964 149-159.
- [24] P. Erdős and L. Moser, P. Erdős, Extremal problems in number theory. 1965 Proc. Sympos. Pure Math., Vol. VIII pp. 181-189 Amer. Math. Soc., Providence, R.I.
- [25] J. Folkman, On the representation of integers as sums of distinct terms from a fixed sequence, *Canad. J. Math.* 18 1966 643-655.
- [26] P. Frankl and Z. Füredi, Solution of the Littlewood-Offord problem in high dimensions. *Ann. of Math.* (2) 128 (1988), no. 2, 259-270.
- [27] G. Freiman, Foundations of a structural theory of set addition. Translated from the Russian. *Translations of Mathematical Monographs*, Vol 37. American Mathematical Society, Providence, R. I., 1973. vii+108 pp.
- [28] G. Freiman, New analytical results in subset sum problem, *Discrete mathematics* 114 (1993), 205-218.
- [29] W. Gao and Y. O. Hamidoune, On additive bases, *Acta Arith.* 88 (1999), no. 3, 233-237.
- [30] W. Gao, Y.O. Hamidoune, A. Llad and O. Serra, Covering a finite abelian group by subset sums, *Combinatorica* 23 (2003), no. 4, 599-611.

- [31] V. Girko, Circle law, (Russian) *Teor. Veroyatnost. i Primenen.* 29 (1984), no. 4, 669–679.
- [32] F. Götze, A.N. Tikhomirov, On the circular law, *preprint*.
- [33] F. Götze, A.N. Tikhomirov, The Circular Law for Random Matrices, *preprint*.
- [34] B. Green, The Cameron-Erds Conjecture *Bull. London Math. Soc.* 36 (2004), no. 6, 769–778.
- [35] B. Green and I. Ruzsa, Freiman’s theorem in an arbitrary abelian group, *Jour. London Math. Soc.* 75 (2007), no. 1, 163–175.
- [36] J. Griggs, J. Lagarias, A. Odlyzko and J. Shearer, On the tightest packing of sums of vectors, *European J. Combin.* 4 (1983), no. 3, 231–236.
- [37] Y. Hamidoune and G. Zémor, On zero-free subset sums, *Acta Arithmetica* 78 (1996) no. 2, 143–152.
- [38] G. Katona, On a conjecture of Erds and a stronger form of Sperner’s theorem. *Studia Sci. Math. Hungar* 1 1966 59–63.
- [39] D. Kleitman, On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors, *Advances in Math.* 5 1970 155–157 (1970).
- [40] E. Lipkin On representation of r -powers by subset sums, *Acta Arithmetica* 52 (1989), 114–130.
- [41] J. E. Littlewood and A. C. Offord, On the number of real roots of a random algebraic equation. III. *Rec. Math. [Mat. Sbornik] N.S.* 12, (1943). 277–286.
- [42] P. Erdős, A. Ginzburg and A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel* 10F (1961), 41–43.
- [43] W. D. Gao, A. Panigrahi and R. Thangadurai, On the structure of p -zero-sum-free sequences and its application to a variant of Erdős-Ginzburg-Ziv theorem. *Proc. Indian Acad. Sci.* Vol. 115, No. 1 (2005), 67–77.
- [44] G. Halász, Estimates for the concentration function of combinatorial number theory and probability, *Period. Math. Hungar.* 8 (1977), no. 3–4, 197–211.
- [45] N. Hegyvári, On the representation of integers as sums of distinct terms from a fixed set, *Acta Arith.* 92 (2000), no. 2, 99–104.
- [46] T. Łuczak and T. Schoen, On the maximal density of sum-free sets, *Acta Arith.* 95 (2000), no. 3, 225–229.
- [47] H. B. Mann and Y. F. Wou, An addition theorem for the elementary abelian group of type (p, p) , *Monatsh. Math.* 102 (1986), no. 4, 273–308.
- [48] M. Nathanson, *Elementary methods in number theory*, Springer 2000.
- [49] H. H. Nguyen, E. Szemerédi and V. Vu, Subset sums in \mathbf{Z}_p , to appear in *Acta Arithmetica*.
- [50] H. H. Nguyen and V. Vu, Classification theorems for sumsets modulo a prime *submitted*.
- [51] H. Nguyen and V. Vu, On square-sum-free sets, *in preparation*.
- [52] J. E. Olson, Sums of sets of group elements, *Acta Arith.* 28 (1975/76), no. 2, 147–156.
- [53] J. E. Olson, An addition theorem modulo p , *J. Combinatorial Theory* 5 1968 45–52.
- [54] G. Pan and W. Zhou, Circular law, Extreme singular values and potential theory, *preprint*.
- [55] A. Sárközy, Finite addition theorems I, *J. Number Theory*, 32, 1989, 114–130.
- [56] A. Sárközy, Finite Addition Theorems, II, *Journal of Number Theory*, 48 (1994), 197–218.
- [57] A. Sárközy and C. Pomerance, Combinatorial number theory, Chapter 20, *Handbook of Combinatorics* (eds. R. Graham, M. Grötschel and L. Lovász), North-Holland 1995.
- [58] A. Sárközy and E. Szemerédi, Über ein Problem von Erdős und Moser, *Acta Arithmetica*, 11 (1965) 205–208.
- [59] R. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Algebraic Discrete Methods* 1 (1980), no. 2, 168–184.
- [60] E. Szemerédi, On a conjecture of Erdős and Heilbronn, *Acta Arith.* 17 (1970) 227–229.
- [61] Endre Szemerédi and V. Vu, Long arithmetic progression in sumsets and the number of x -free sets, *Proceeding of London Math Society*, 90(2005) 273–296.
- [62] E. Szemerédi and V. Vu, Finite and infinite arithmetic progression in sumsets, *Annals of Math*, 163 (2006), 1–35.
- [63] E. Szemerédi and V. Vu, Long arithmetic progressions in sumsets: Thresholds and Bounds, *Journal of the A.M.S.*, 19 (2006), no 1, 119–169.
- [64] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Univ. Press, 2006.
- [65] T. Tao and V. Vu, Random matrices: The Circular Law, *Communication in Contemporary Mathematics* 10 (2008), 261–307.
- [66] T. Tao and V. Vu, Inverse Littlewood-Offord theorems and the condition number of random matrices, to appear in *Annals of Mathematics*.

- [67] T. Tao and V. Vu, *paper in preparation*.
- [68] V. Vu, Structure of large incomplete sets in abelian groups, *to appear in Combinatorica*.
- [69] Wigner, On the distribution of the roots of certain symmetric matrices, *Annals of Mathematics* (2) 67 1958 325–327.

DEPARTMENT OF MATHEMATICS, RUTGERS, PISCATAWAY, NJ 08854

E-mail address: `vanvu@math.rutgers.edu`